Trends and Developments in Telecommunication Security

Duminda Wijesekera
Department of Information and Software Engineering
George Mason University, Fairfax VA 22030.
703-993-1578
dwijesek@gmu.edu

Abstract

SS7 is a signaling system for the public switched telephone network (PSTN) [1,2,3]. SS7 network transports call setup, teardown messages, database queries, trunk status, instructions for remote phone switches and so on, in fact it acts as a glue for the circuit switched networks. Before the deregulation act it was envisioned as a closed community network. After the deregulation, landscape has changed; the emerging environment includes convergence of telephone, IP and wireless networks. The convergence results in increasing number of interfaces between SS7 and other networks, and each brings with it many vulnerabilities. Every point at the interface is a potential point of attack.

1. SS7 Network Security

With the increasing number of telecommunication service providers with different levels of experiences, skills and ethics, it is becoming more important to protect signaling network. We have the access of new and more powerful equipments which have the capability of generating custom messages and put into numerous available entry points at interfaces between SS7 and IP or mobile networks. As per Telcordia specification (GR-82-CORE) [8] some screening capability is employed at the Signaling Transfer Points (STPs) because STPs provide a view to the internal network and provide a venue to gather valuable information. This capability is referred as a Gateway Screening capability. Major STP vendors have incorporated Gateway Screening capability in their products. This screening capability screens MTP [2] message headers and if the message type is Network Management Message then it checks content of the message. Gateway Screening checks the *origination point code (OPC)* [i.e. sender's address] and *destination point code (DPC)* [receiver's address] of the message to determine whether this is allowed into the network. Since Gateway Screening does not check the content of the other higher protocols of SS7 (such as ISUP, TCAP) [1,2,3], responsibility falls upon the Service Switching Points (SSPs) and this may cause problem at the switch affecting all the services [1].

As the number of interfaces increases, the attack points and types of attacks are also increasing. We are facing with the problems in message format or structure, message content, spoofing and sniffing problems. Depending upon the threats persisting in today's SS7 network it can be classified into three different broad categories:

a) Threats related to loss of integrity of signaling data and resources

Integrity of data means that the data have not been altered or destroyed in an unauthorized manner in the process of communication. The protection of the SS7 includes the protection of routing data and other relevant information that can be altered using particular signaling messages. To this class of threats belong:

- routing reconfiguration
- traffic diversion
- isolation of a user part
- Isolation of a specific node in the network.

b) Threats related to masquerading and unauthorized access

Before having access to a network, or a specific machine in this network, an entity must identify itself and the network protection then authenticates this entity. These identification and authentication procedures may be performed at various stages of the communication process. The common case in the signaling network is the sending of messages that are not authorized to go through the network they are entering or are not authorized to use a particular signaling service. To this class of threats belong:

- congestion
- modification of the status of a remote subsystem
- Sending of signaling traffic to non available signaling point.

c) Threats related to eavesdropping and disclosure of sensitive information

Confidentiality of data means that the data have not been disclosed, in the process of communication or while being stored without the permission of its owner. To this class of threats belongs:

- Prohibition and inability of a user to access a particular service.

The risks of all these intentional or accidental threats including corruption, disclosure, loss or removal of resources are the misuse of data or resources.

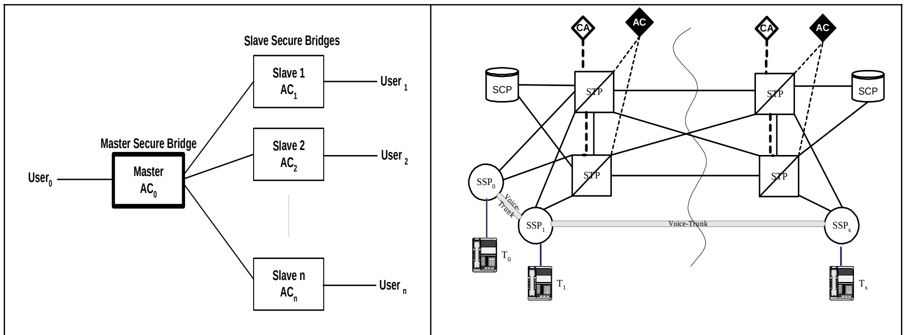
Ongoing Research Projects

Voice Privacy

1.) The main objective is to propose a security architecture that provides end-to-end voice privacy at the application layer with minimum modification of existing public telephone network infrastructures. Voice privacy is achieved by encrypting voice signals between two end telephones using symmetric keys and a one-time encryption key. This one-time encryption key is used to prevent replay attacks. The security architecture also proposes imposing an access control mechanism for telephone subscribers and telephones that are to be used for secure communications. Proposed authentication technique uses public key cryptography and provides authentication center the assurance that the telephone at the other end of the connection is what it claims to be.

2.) Two-way group voice communications, otherwise known as teleconferencing are common in commercial and defense networks [4,5,6]. One of the main features of military teleconferences is the need to provide means to enforce the Multilevel Security (MLS) model. In this paper we provide architecture and protocols facilitating MLS conferences over Public

Switched Telephone Network (PSTN), protecting the confidentiality needs of the conversation. We develop protocols to establish secure telephone conferencing at a specific security level, add and drop conference participants, change the security level of an ongoing conference, and tear down a conference. These protocols enforce MLS requirements and prevent eavesdropping. . Our solution is based on encryption methods used for user and telephone authentication and message encryption, and trusted authentication centers and certificate authorities.



The control structure of the secure teleconferencing	Secure teleconferencing architecture

Figure 1: Developed Secure Teleconferencing Architecture

In addition, the research investigates how to integrate the proposed security architecture with PSTN and wireless networks call process model, and the effect of voice quality on the effectiveness of secure call. The proposed security architecture will be implemented at the application service elements (ASE) layer of the SS7 protocol model, where existing security architectures and other advanced intelligent network services in the wire-line and wireless network are being implemented.

<u>Tangible Resulting of this Effort:</u>

[1] Mohamed Sharif and Duminda Wijesekera, In Proceeding of the 10th International Conference on Telecommunication Systems: Modeling and analysis, October 3-6, 2002, Monterey, CA, USA, Page 214-224

[2] Mohamed Sharif and Duminda Wijesekera, In Proceeding of IFIP TC11 18th International Conference on Information Security (SEC2003) May 26-28, 2003, Athens, Creece, Page 25-36

[3] Inja Youn and Duminda Wijesekera, Secure Bridges: A means to conduct secure teleconferences over public telephones, Proc. 18th IFIP WG 11.3 Working Conference on Data and Application Security, Sitges , Spain , July 2004

[4] I. Youn, C. Farkas, B. Thuraisingham, Multilevel Secure Teleconferencing over Public Switched Telephone Network, Proc. IFIP 19th WG 11.3 working conference on Data and Application Security, August, 2005

[5] Mohamad Sherif, Duminda Wijesekera and James Bret Michael, A method to provide end-to-end voice privacy as well as telephones and subscribers authentication with minimum modification to existing public telephone network infrastructures. Patent application in process at the GMU patent office.

[6] Inja Youn, Duminda Wijesekera and Csilla Farkas, Secure Bridges: A design and algorithms for Secure Conference Calling privacy as well as telephones and subscribers authentication with

minimum modification to existing public telephone network infrastructures. Patent application in process at the GMU patent office.

Spoofing Threat

SS7 network presently interfaces with many other networks and each point of attachment presents a viable entry point to the signaling network. Anyone who is capable of generating SS7 messages and introducing it into SS7 network can bring down the telephone services. For example, intruder or attacker can create harmful messages by fabricating ISUP messages and introducing them into the network by using ISDN access points. ISUP messages are responsible for call setup and teardown so any fabrication can create havoc in the network. Other example of the spoofing threat may be that one client connected to a SS7 network can send its own traffic as it came from another client. In the signaling network there is no authentication process to ensure the validity of the transmitting nodes outside of the network boundary. Here we are proposing a solution at the MTP3 (Message Transfer Part Level 3) layer in the SS7 protocol stack which can perform authentication process to make sure the validity of the nodes which lie outside of the network perimeter.

Tangible Results of this Effort :

[1] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: Authentication and Integrity in Telecommunication Signaling Network. IEEE ECBS 2005: 163-170
[2] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network. IEEE IPDPS 2005

Current Trends: Integrating PSTN and IP Networks

IP telephony, commonly known as Voice over IP (VoIP) is emerging as a viable alternative to traditional wired line and wireless telephone systems. Recent days many companies are coming-up to provide telephony services over Broadband networks. Before it presents a real formidable challenge to existing public switched telephone network (PSTN), it has to solve two main challenges, quality of service (QoS) and security issues. QoS has already received considerable efforts from academia and industry. Only recently, security of VoIP is being discussed and raised some interest in the industry while academia is still lagging behind. As the popularity of VoIP and its deployment grows, they are fast becoming the targets of spammers, hackers and crackers. VoIP calls and internet traffic share the same path and are prone to same type of risks of data networks. On the other hand voice service brings along with it many new forms of vulnerabilities affecting itself and existing data networks. Known solutions, that were designed to address security vulnerabilities of data networks falls short of defending voice application. VoIP systems use multiple protocols for call control and data delivery. For example, in SIP based IP telephony, Session Initiation Protocol (SIP) is used to control call setup and teardown and Real time Transport Protocol (RTP) for media delivery. VoIP systems are distributed in nature, consisting of IP phones, SIP proxies and many other servers. To defend against attacks on such a heterogeneous and distributed environment, we need to incorporate communication between protocol state machines. Call control and media delivery protocols are synchronized by exchanging synchronization message for critical events throughout the established session. VoIP deployment suffers threats from many different network layers, besides protocol layers vulnerabilities other possible sources of attacks could be:

1. Mis-configuration of devices
2. Vulnerability of its underlying operating system.
3. Protocol implementation flaw.
4. Well-known attacks of data networks such as worms, viruses, Trojan horse, DoS.
5. Protocol translation at the Interface between PSTN and IP nodes.

Architecture:

Voice over IP (VoIP) is emerging as a viable alternative to traditional wired line and wireless telephone systems, commonly referred to as public switched telephone networks (PSTN). They have different networking architectures. For example, VoIP uses IP, a packet switched network and PSTN uses a circuit switched network where a signaling network known as the signal system 7 (SS7) sets up connections for voice lines. Nevertheless, as shown in Figure, they interoperate making it possible to pick up a phone in either network and call another phone in the other network. In order to facilitate this interoperability, IETF's SIGTRAN RFC:2719 working group has defined an architecture for SS7 to interwork with IP network through a gateway that interface between the two. This gateway translates the networking protocols on one side over the other. Despite many advantages, one of the disadvantages of interoperating VoIP and SS7 is that one of them could be used as an entry point to disrupt the functionality of the other.

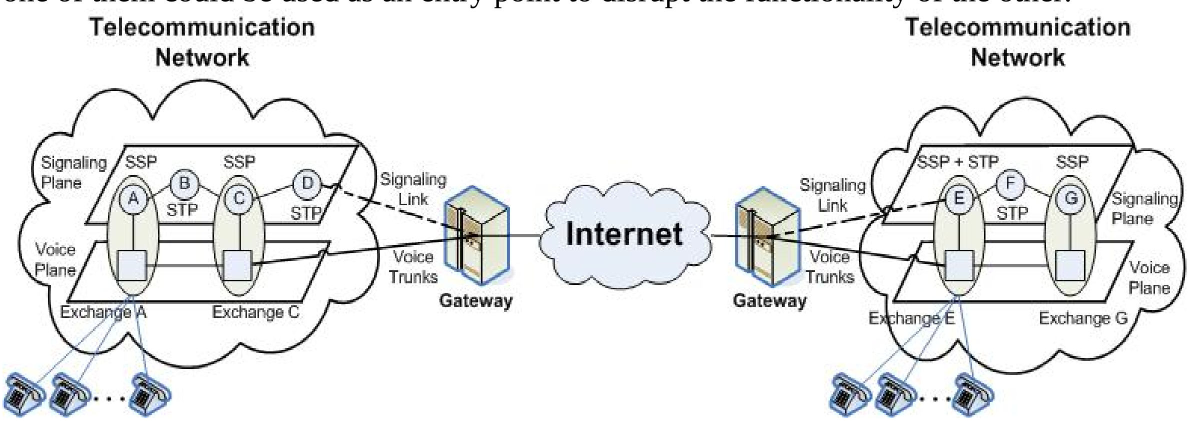


Figure 2: Interoperating Architecture for SS7 and VoIP

Inside the Internet or IP network, we could use SIP based IP telephony. SIP is a text based application level protocol for set-up, modify and tear down of multimedia sessions between one or more participants. SIP identifies two basic types of components, one is SIP user agent and the other is various SIP servers. Thus giving an attacker, a wide range of target devices, starting from end devices such as IP phones to Routers, Switches, Signaling Gateways, Media Gateways and SIP Proxies. In fact any device in the path from caller to callee can be an attacker's target. We describe some of the vulnerabilities existing at the interface between PSTN and IP network, and in IP network itself.

Ongoing Research Projects

Vulnerabilities at the interface between PSTN and IP Network :

Currently VoIP and PSTN interoperate with each other, where a signal that originates in one may go over a series of VoIP or PSTN network and terminate in a destination situated in either one of them. Telecommunication deregulation act of 1996 in the USA and liberalization of economies have introduced new and yet to be trusted signaling entities. Any body with a different level of experience and ethics can become a competitive local exchange carriers (CLECs) and hence have the ability to generate SS7 messages. To reap the benefits of IP network, CLECs will also be encouraged to attach themselves to IP network. Thus the threats arising to signaling nodes are two fold, it may either come from SS7 or from IP network. In this integrated signaling network architecture threats may arise due to message content or structure, due to traffic flow analysis, misbehaving signaling nodes in IP network, violation of protocol state machine and exploitation of signaling network management messages.

Tangible Results of this Effort:

[1] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: Gateway Security for SIGTRAN's M3UA protocol in VoIP Networks. IEEE GLOBECOM, Workshop on VoIP Security Challenges and Solutions 2005
[2] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia, Ram Dantu: Securing VoIP from Signaling Network Vulnerabilities. "submitted to a conference".

Vulnerabilities to SIP based IP Telephony :

SIP stacks can be found on PCs, laptops, VoIP phones, mobile phones and wireless devices. To facilitate the interconnection between these end devices, SIP uses SIP Gateways and SIP Servers. Attackers have a range of target devices, starting from end devices such as IP phones to Routers, Switches, Signaling Gateways, Media Gateways and SIP Proxies. Any of these targeted device could be attacked at different levels (or layers) of network protocol. At the transport layer, responsible for the transmission of SIP signaling messages and media stream, is susceptible to TCP SYN flooding and UDP flooding attacks. At the application layer, SIP is prone to INVITE flooding attacks and RTP is RTP packets flooding attacks. Distributed denial of service attacks against SIP could also be launched using reflectors. Besides of these flooding denial of service attacks, SIP based IP telephony may also become the target of session hijacking, media spamming and fraud.

Tangible Outputs of this Effort:

[1] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: VoIP Intrusion Detection and Prevention using Communicating Protocol State Machines. "submitted to a conference".

References

[1] J. G. von Bosse. Signaling in Telecommunication Networks. John Wiley & Sons, New York, 1998.

[2] Specifications of Signaling System No. 7--Message Transfer Part Signaling Performance. ITU-T Recommendation Q.706, March 1993.

[3] Specifications of Signaling System No. 7--Signaling performance in the Telephone Application. ITU-T Recommendation Q.706, March 1993.

[4] Stage 3 description for multiparty supplementary services using DSS 1. ITU-T Recommendation, Q.954, 1993.

[5] Stage 3 description for multiparty supplementary Specifications of signaling system no. 7. ITU-T Recommendation Q.734, 1993.

[6] Stage 2 description for multiparty supplementary services. ITU-T Recommendation Q.84, 1993.

[7] Specifications of Signaling System No.7--Hypothetical Signaling Reference Connection. ITU-T Recommendation Q.709, March 1993.

[8] Telecordia GR82-CORE, available at http://telecom-info.telcordia.com/ido/AUX/GR_82_TOC.i08.pdf

[9] Mohamed Sharif and Duminda Wijesekera, In Proceeding of the 10th International Conference on Telecommunication Systems: Modeling and analysis, October 3-6, 2002, Monterey, CA, USA, Page 214-224

[10] Mohamed Sharif and Duminda Wijesekera, In Proceeding of IFIP TC11 18th International Conference on Information Security (SEC2003) May 26-28, 2003, Athens, Creece, Page 25-36

[11] Inja Youn and Duminda Wijesekera, Secure Bridges: A means to conduct secure teleconferences over public telephones, Proc. 18th IFIP WG 11.3 Working Conference on Data and Application Security, Sitges , Spain , July 2004

[12] I. Youn, C. Farkas, B. Thuraisingham, Multilevel Secure Teleconferencing over Public Switched Telephone Network, Proc. IFIP 19th WG 11.3 working conference on Data and Application Security, August, 2005

[13] Mohamad Sherif, Duminda Wijesekera and James Bret Michael, A method to provide end-to-end voice privacy as well as telephones and subscribers authentication with minimum modification to existing public telephone network infrastructures. Patent application in process at the GMU patent office.

[14] Inja Youn, Duminda Wijesekera and Csilla Farkas, Secure Bridges: A design and algorithms for Secure Conference Calling privacy as well as telephones and subscribers authentication with minimum modification to existing public telephone network infrastructures. Patent application in process at the GMU patent office.

[15] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: Authentication and Integrity in Telecommunication Signaling Network. IEEE ECBS 2005: 163-170

[16] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: MTPSec: Customizable Secure MTP3 Tunnels in the SS7 Network. IEEE IPDPS 2005.

[17] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: Gateway Security for SIGTRAN's M3UA protocol in VoIP Networks. IEEE GLOBECOM, Workshop on VoIP Security Challenges and Solutions 2005

[18] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia, Ram Dantu: Securing VoIP from Signaling Network Vulnerabilities. "submitted to a conference".

[19] Hemant Sengar, Duminda Wijesekera, Sushil Jajodia: VoIP Intrusion Detection and Prevention using Communicating Protocol State Machines. "submitted to a conference".